COTS Installation Instructions
– Sun ONE Directory Server 5.2 –

1. Prerequisites

- Solaris 8 with ECS baseline patches
- 256MB memory and 3GB disk space on internal disk
- Netscape 4.78 browser
- The following tar file:

Checksum	Size	Name
1127661478	71023616	SunOne_LDAP_Server_5.2.tar

- Access to the following Sun ONE Directory Server manuals, available at http://docs.sun.com/db/coll/S1_DirectoryServer_52:
  - Getting Started Guide
  - Installation and Tuning Guide
  - Administration Guide
  - Server Management Guide
  - Deployment Guide
  - Release Notes
- The basic information required during installation (see Table 1 below):

Table 1. Directory Server Installation Worksheet

Description	Examples
Administration domain	`<local domain name>` (e.g., example.com)
Administration Server port number	`<port #>`
Directory Administrator ID	`admin`
Directory Administrator password	`<password>`
Directory Manager DN [1] (super user for the directory)	`cn=Directory Manager`
Directory Manager password (at least 8 characters)	`<password>`
Directory Server port number (1-65535,inclusive)	`389` (default LDAP) `636` (default LDAP/SSL)
Fully qualified host distinguished name	`g0css02.gsfcb.ecs.nasa.gov`
Server ID (No periods or spaces allowed)	`g0css02`
Server suffix (At least one to hold directory content)	`dc=gsfcb,dc=ecs,dc=nasa,dc=gov`
ServerRoot (software installation directory)	/usr/ecs/OPS/COTS/dirsrvr52
(Do not install on top of an existing earlier version. Do not install Sun ONE Web Server in the same *ServerRoot* as Directory Server.)	
(UNIX platforms) Server group ID Use the name, rather than the group ID number.	`noaccess`
(UNIX platforms) Server user ID Use the name, rather than the user ID number.	`diruser`

2. Uninstall instructions

None

3. Installation Instructions

3.1 Prepare for Installation

1) Become superuser on the designated directory server machine, g0css02

2) Obtain and place the files in a staging directory such as /tmp/install:

```
# mkdir /tmp/install
# cp SunOne_LDAP_Server_5.2.tar /tmp/install
# cd /tmp/install
# tar xvf SunOne_LDAP_Server_5.2.tar
# cp slapd /etc/init.d/
# cp slapd /etc/rc2.d/S80slapd
# cp slapd /etc/rc1.d/K15slapd
# chmod 744 /etc/init.d/slapd
# chmod 744 /etc/rc2.d/S80slapd
# chmod 744 /etc/rc1.d/K15slapd
```

3) Create the destination directory:

```
# mkdir –p /usr/ecs/OPS/COTS/dirsrvr52
```

4) Unpack the tarfile:

```
# cd /tmp/install
# gunzip directory-5.2-us.sparc-sun-solaris2.8.tar.gz
# tar xvf directory-5.2-us.sparc-sun-solaris2.8.tar
```

5) Run the idsktune utility to check for appropriate patches and system tuning:

```
# ./idsktune –q > /tmp/idsktune.out
# cat /tmp/idsktune.out
```

6) Note the output from the command. Items marked with NOTE or WARNING can be ignored but any marked with ERROR will need to be corrected before proceeding. Contact the Landover help desk as necessary.

7) Create a new local user and group for use with the LDAP server:

```
# /usr/sbin/useradd -c "Directory User" -u 60003 -g noaccess -s /bin/sh \
-d /dev/null diruser

# vi /etc/group, and add diruser to the noaccess group
```

3.2 Install Sun ONE Directory Server

1) Start the install script:

```
# cd /tmp/install
# ./setup –nodisplay
```

Note: In the remainder of the installation the script will suggest a default in brackets. If the default is correct, you only need to press ENTER to continue. Otherwise, you will need to correct the suggested default.

Note: The below is an extract of the installation dialog highlighting responses to make.

2) Press ENTER through the prompts as you read the license data until you are prompted with:

```
Have you read, and do you accept, all of the terms of the preceding Software
License Agreement [no] {"<" goes back, "!" exits}?
```

(Type "**yes**" and press **ENTER**.)

3) At the next prompt, ensure that the correct fully qualified hostname is displayed, then either press ENTER (↵) or type name

Fully Qualified Computer Name [hostname.domain.com] {"<" goes back, "!" exits}:

4) Select what to install:

```
Choose the type of installation from the following choices:

Sun ONE Servers - Installs the Sun ONE servers, Sun ONE Server Console, and
related components.

Sun ONE Server Console - Installs the Sun ONE Server Console as a stand-
alone
Java application.

1. Sun ONE Servers
2. Sun ONE Server Console

   What would you like to do [1] {"<" goes back, "!" exits}?
```

(Select **1**)

5) Select type of installation:

```
Choose the type of installation you prefer from the following choices:

Express - Installation option choices are made automatically. The easiest
installation and recommended for evaluating the product.
Typical - Software will be installed with the most common options.
Recommended
for most deployments.

Custom - You may choose the options you want to install. Recommended for
advanced users.

1. Express
2. Typical
3. Custom

   What would you like to do [2] {"<" goes back, "!" exits}?
```

(Select Custom by typing "**3**")

6) Enter the installation directory:

```
The Directory Server components will be installed in the following
directory.
Specify the directory location where you want to install the product.

   Directory to install Directory Server components into [/var/Sun/mps] {"<"
```

```
   goes back, "!" exits}:
```

(Enter: **/usr/ecs/OPS/COTS/dirsrvr52**)

Files are copied to the directory. Can take several minutes.

7) Verify components to be installed:

```
Directory Server components showing a checked box will be installed.

 [X]  1   Sun ONE Directory Suite    0 bytes
 [X]  2     Sun ONE Directory Server    27.35 MB
 [X]  3     Sun ONE Directory Server (64-bit support)    37.03 MB
 [X]  4     Sun ONE Directory Console Support    1.74 MB
 [X]  5   Sun ONE Administration Services    0 bytes
 [X]  6     Sun ONE Administration Server    11.45 MB
 [X]  7     Sun ONE Administration Console    227.78 KB
 [X]  8   Sun ONE Server Console    0 bytes
 [X]  9     Sun ONE Server Console Core    6.72 MB
 [X]  10    Java Runtime Environment    65.00 MB
 [X]  11  Sun ONE Server Basic Libraries    26.55 MB

   To check a particular component, enter its number, or 0 when you are
   finished [0] {"<" goes back, "!" exits}:
```

(Enter **0** to select all components and proceed)

8) Enter the system user and group:

```
Choose the system user and group names under whose identity
the Sun ONE Directory server will run.

   System User [root] {"<" goes back, "!" exits}:
```

(Enter “diruser” for user)

```
   System Group [other] {"<" goes back, "!" exits}:
```

(Enter “**noaccess**” for group)

9) Existing configuration or new configuration:

```
You may store Sun ONE server configuration information in another Sun ONE
Directory Server. If you have already prepared a configuration server, you
may configure the new server to use it.

1. The new instance will be the configuration Directory Server
2. Use existing configuration Directory Server

   What would you like to do [1] {"<" goes back, "!" exits}?
```

(Enter **1**)

10) Store user and group information in the new Directory Server?:

```
You may already have a Directory Server where you store user and group
information.

1. Store data in the new Directory Server
2. Store data in an existing Directory Server
```

```
   What would you like to do [1] {"<" goes back, "!" exits}?
```

(Enter **1**)

11) Enter server settings:

```
Settings the new server will use for basic operation

   Server Identifier [hostname] {"<" goes back, "!" exits}:
```

(Verify the default, or enter the "short" hostname – hostname minus domain (e.g., g0css02)

```
   Server Port [389] {"<" goes back, "!" exits}:
```

(Accept the default of 389)

```
   Suffix [dc=gsfcb, dc=ecs, dc=nasa, dc=gov] {"<" goes back, "!" exits}:
```

(Verify the default, or enter the ***domain portion of the hostname*** in the format above)

12) Enter Directory Server Administrator login info:

```
Configuration Directory Server Administrator

   Administrator ID [admin] {"<" goes back, "!" exits}:
```

(Accept "admin" for the ID)

```
Password:
Password (again):
```

(Enter and verify the ***admin password***)

13) Enter the administration domain:

```
Administration Domain

   Administration Domain [gsfc.nasa.gov] {"<" goes back, "!" exits}:
```

(Verify the default or enter the hosts's ***domainname***)

14) Enter the Directory Manager's Distinguished Name:

```
Enter a Distinguished Name (DN) for the Directory Manager and a password at
least 8 characters long.

   Directory Manager DN [cn=Directory Manager] {"<" goes back, "!" exits}:
```

(Accept the default "Directory Manager" for the DN)

```
Password:
Password (again):
```

(Enter and verify the ***Directory Manager password***)

15) Populate with data?

```
You may populate the suffix of the new Directory Server instance from an
LDIF file, or create sample data in your suffix.

1. Don't populate
2. Populate with sample data
```

```
3. Populate with LDIF file

   What would you like to do [2] {"<" goes back, "!" exits}?
```

(Enter **1**, "Don't populate")

16) Set Administration Port:

```
The Administration Server runs on a different network port from other
servers.
Specify the number of the port.

   Administration Port [390] {"<" goes back, "!" exits}:
```

(Enter an unused ***port number***, preferably one (1) greater than that specified for the iPlanet Administrator Server. Refer to your worksheet in Table 1.)

17) Verify and begin installation:

```
Ready to Install

1. Install Now
2. Start Over
3. Exit Installation

   What would you like to do [1] {"<" goes back, "!" exits}?
```

(Enter "**1**" to Install Now)

18) Confirm Installation:

```
Installation Details:

     Product           Result     More Information
 1.  Directory Server  Installed  Available

 2. Done

   Enter the number corresponding to the desired selection for more
   information, or enter 2 to continue [2] {"!" exits}:
```

(Enter "**2**" to continue)

Note: Initial installation is complete!

19) Stop and restart the server.

```
# /etc/init.d/slapd stop
# /etc/init.d/slapd start
```

20) Clean up any files in /tmp that are no longer needed.

21) Backup the LDAP directory tree. A uniquely named backup file will be placed in the /usr/ecs/OPS/COTS/dirsrvr52/slapd-<host name>/bak directory:

```
# /usr/ecs/OPS/COTS/dirsrvr52/slapd-<host name>/db2bak
```

NOTE: To restore data, use "…/bak2db <*backup directory*>".

IMPORTANT: Instructions that follow require that cookies be enabled in your web browser!

3.3 Configure iPlanet Web Server to Use the Directory Server

These and the other instructions below configure the iPlanet web server on the SSS GUI machine only. However, they can be readily adapted to protect web-based resources on other iPlanet machines as well.

1) Log on the SSS GUI host as root.

2) Backup the web server's ACL/LDAP database mapping file:

3) From a Netscape browser on any host, access the iPlanet Administration Server for the SSS GUI host by entering the appropriate URL and port number (e.g., <*host*>.<*domain*>:<*administration server port*>).

4) Enter the Administration Server's **userid** and **password**.

5) Choose the **Global Settings** tab. The Configure Directory Service page appears.

6) Enter the following values:

`Host Name:`	<***directory server's IP address*** or ***host name***> (e.g., g0css02.gsfcb.ecs.nasa.gov)
`Port:`	***<directory server port #>*** (i.e., the value entered in step 16 of Section 3.2)
`Sockets Layer (SSL) for connection?:`	**No**

Click **OK** to change your port to the standard port for LDAP over SSL.

`Base DN:`	**dc=<*domain comp 1*>,dc=<*domain comp 2*>,** … (e.g., "dc=gsfc,dc=ecs,dc=nasa,dc=gov" – no spaces)
`Bind DN:`	**cn=Directory Manager**
`Bind Password:`	***<Directory Manager's password>***

7) Click **Save Changes**, then click **OK** to acknowledge that you must shut down and restart the Administration Server and all the servers it is managing.

8) As root at a Unix prompt on the SSS GUI machine, stop and start the Administration Server as follows:

```
# /etc/init.d/iplanetadm stop
# /etc/init.d/iplanetadm start
```

9) Restart all Web Server instances.

   a) Click the **Servers** tab.

   b) Select an instance using the "Select a Server" dropdown list, then click **Manage**. The Server On/Off page appears.

   c) Click **Server Off**. Click **OK** to acknowledge the prompt, then click **Server On**.

   d) Select the next instance using the dropdown list at the top of the GUI, and repeat step c. Do this for each remaining web server instance.

   e) Using the dropdown list at the top of the GUI, select **Web Server Administration Server** to return to the Manage Servers page.

3.4 Create New User Entries using iPlanet Web Server

You can use the iPlanet Administration Server to add users to the Directory Server database.

1) At the Manage Servers page in your Netscape browser, choose the **Users & Groups** tab. The New User page appears.

2) Enter the following minimum information on the displayed page:

Given Name:	<***first name***>	
Surname:	<***last name***>	(required field)
User ID:	<***userid***>	(required field)
Password:	<***password***>	
Password (Again):	<***password***>	

Add New User To: select **People** from dropdown list

For more information, see the New User page in the online help.

3) Click **Create User** to create the user entry. A fresh New User page appears.

4) Repeat steps 3-4 to create additional users.

NOTE: If you need to delete a user entry, perform the following steps:

1) Access the Administration Server, choose the **Users & Groups** tab, and click the **Manage Users** link.

2) In the Find User field, enter some ***<descriptive value>*** for the entry, such as name or user ID, then click **Find**.

3) Click the ***<name of the user>*** that you want to edit.

4) Click **Delete User**.

For more information, see The Manage Users page in the online help.

3.5 Create a New (Static) Group using iPlanet Web Server

You can use the iPlanet Administration Server to add user groups to the Directory Server database.

1) At the New User page in your Netscape browser, click the **New Group** link. The New Group page appears.

2) Enter the following minimum information on the displayed page:

Type of Group:	**New Group**
Group Name:	<***group name***> (e.g., SSS Managers)
Description:	**People who can manage Spatial subscriptions**
Add New Group To:	select **Groups** from dropdown list

3) Click **Create and Edit Group** to create the group. The Edit *group name* page appears.

4) In the Group Members field, click **Edit**. The Edit Group Members page appears.

5) In the field “matching”, enter a ***<name>*** or ***<user ID>*** -- you can use wildcard chars. such as (*) -- then click **Find and Add**. If found, matching user IDs are displayed in the lower pane on the page. If none are found, correct your entry and try again (using wildcard chars. if helpful).

6) Repeat step 5 to add additional group members.

7) Click **Save Changes**. The Edit *group name* page appears.

8) Click **Save Changes,** again.

9) Click the **Servers** tab to return to the Manage Servers page.

NOTE: For more information, see the New Group page in the online help.

3.6 Configure iPlanet Web Server To Protect SSS GUIs

You can create, edit, or delete access control for a specific server instance using the Administration Server's Server Manager GUI. You will need to configure three web server instances, one for each mode in which the SSS GUI runs. The instructions below start you with the server instance for TS2 mode.

IMPORTANT: The custom code to be protected must have already been installed!

1) Using the "Select a Server" dropdown list on the Server Manager page of your Netscape browser, select the **SSS web server instance for TS2 mode** (e.g., g0dps01_SSS_TS2), then click **Manage**.

2) As root on the SSS GUI machine, backup the server's two ACL files:

```
# cd /usr/ecs/OPS/COTS/www/iplanet/servers/httpacl/
# cp  genwork.https-g0dps01_SSS_TS2,acl    genwork.https-g0dps01_SSS_TS2.acl.bak
# cp  generated.https-g0dps01_SSS_TS2.acl  generated.https-g0dps01_SSS_TS2.acl.bak
```

NOTE: The above is just a precaution. When you use the Administration Server to edit ACL files, it should automatically place a backup copy in the web server instance's conf_bk directory. The file will have an acl.*n* suffix.

3) Click the **Restrict Access** link.

4) Click **OK** to edit the default ACL file. The Access Control List Management page appears.

5) Protect your TS2 mode resources by performing the steps below for each resource, such as "/usr/ecs/TS2/CUSTOM/WWW/SSS/cgi-bin/EcNbAddBundle.pl".

   a) On the Access Control List Management page, click Pick a Resource's **Browse** button. The Choose a Part of Your Server page appears.

   b) Click on **Options**.

   c) Change the value in the List From field from "/usr/ecs/TS2/CUSTOM/SSS/docs" to "**/usr/ecs/TS2/CUSTOM/SSS/cgi-bin**".

   d) Click **List files as well as directories**, then click **OK**.

   e) Click on a ***<file name>*** to protect. The Access Control List Management page returns.

   f) Click on "Pick a resource's" **Edit Access Control** button. The Access Control Rules page appears, and it contains no rules.

   g) Add two rules to the Access Control Rules page – one to deny access to anyone, and a second to allow access to members of the SSS Managers group:

      i) Click **New Line** to add a new access control rule. A *Deny anyone* rule appears.

      ii) Click **New Line** again to add a second rule – this one for your authorized user group. Another *Deny anyone* rule appears.

      iii) Change *Deny* to *Allow* in rule 2 by clicking on **Deny**. The Allow/Deny page appears. Select **Allow**, then click **Update** to close the page.

      iv) Change *anyone* to <*group_name*> in rule 2 by clicking on **anyone**. When the User/Group page appears, enter **SSS Managers** in the Group field. (You can use the **List** button to check the group names in the LDAP database.) Select **Default** as the Authentication method and Authentication Database. Click **Update** to close the page.

      NOTE: Be sure to click Update!

v) To adjust access rights for the grou, click on **all** in the Rights column. The Access Rights page appears. Select the desired rights, then click **Update** to close the page.

NOTE: Be sure to click Update!

vi) Ensure that **Continue** is selected for both rules.

vii) Ensure that **Access control is on** is selected.

viii) Click **Submit** to store the rules in the appropriate ACL work file. This also closes the Access Control Rules page. The work file is: /usr/ecs/OPS/COTS/www/iplanet/servers/httpacl/genwork.https-g0dps01_SSS_TS2.acl.

ix) Click the **Apply** button at the upper right-hand side of the Server Manager GUI to update the operational ACL file: /usr/ecs/OPS/COTS/www/iplanet/servers/httpacl/generated.https-g0dps01_SSS_TS2.acl.

x) At the prompt, click **Apply Changes**, then click **OK** to acknowledge that the server started.

h) Repeat steps a-g for each additional TS2 mode resource/file you want to protect.

6) Now do TS1 mode. Using the dropdown list at the top of the GUI, select the **SSS web server instance for TS1 mode** (e.g., g0dps01_SSS_TS1) and repeat steps 2-5 substituting TS1 for TS2.

Note: As an alternative, you could copy the two, TS2-mode ACL files into TS1-mode's ACL files, edit them to protect the TS1 paths, and restart TS1 mode's web server instance. See the sample file in Appendix A.

7) Now do OPS mode. Using the dropdown list at the top of the GUI, select the **SSS web server instance for OPS mode** (e.g., g0dps01_SSS_OPS) and repeat steps 2-5 substituting OPS for TS2.

4. Interrogation Checkout

None

5. Backout Instructions

To remove the Sun ONE Directory Server, Server Console, and Administration Server:

1) As root on the SSS GUI host, g0dps01, de-couple the Web servers from the Directory Server by restoring the dbswitch.conf and default ACL files:

```
# cd /usr/ecs/OPS/COTS/www/iplanet/servers/httpacl/
# cp genwork.https-g0dps01_SSS_<mode>,acl.bak   genwork.https-g0dps01_SSS_<mode>.acl
# cp generated.https-g0dps01_SSS_<mode>.acl.bak generated.https-g0dps01_SSS_<mode>.acl
```

2) Restart the Admin Server:

```
# /etc/init.d/iplanetadm stop
# /etc/init.d/iplanetadm start
```

3) Restart all Web Server instances.

a) At the Web Server Administration Server GUI, click the **Servers** tab.

b) Select an instance using the "Select a Server" dropdown list, then click **Manage**. The Server On/Off page appears.

c) Click **Server Off**. Click **OK** to acknowledge the prompt, then click **Server On**.

d) Select the next instance using the dropdown list at the top of the GUI, and repeat step c. Do this for each remaining web server instance.

4) As root on the Directory Server host, g0css02, uninstall Directory Server:

```
# cd /usr/ecs/OPS/COTS/dirsrvr52
# ./uninstall_dirserver
```

Follow the instructions on each screen. If the uninstallation program cannot remove all files, it displays a message. Manually remove the remaining files.

Appendix A

```
version 3.0;
acl "es-internal";
allow (read, list, execute,info) user = "anyone";
deny (write, delete) user = "anyone";

acl "test";

authenticate (user,group) {

        database = "default";

        prompt = "test access";

};

deny (all)

 (user = "anyone");



allow (all)

 (user = "<user ID>");



acl "default";
authenticate (user,group) {
        database = "default";
        prompt = "iPlanet Web Server";
};
allow (read,execute,list,info)
 (user = "anyone");

allow (write,delete)
 (user = "all");

acl "path=<fully qualified file name 1>";
authenticate (user,group) {
        database = "default";
        method = "basic";
};
allow (all)                                    (grants named user full privileges to file)
 (user = "<user ID>");

acl "path=<fully qualified file name 2>";
authenticate (user,group) {
        database = "default";
        method = "basic";
};
deny (all)                                     (disallows access to file for everyone…
 (user = "all");

allow (all)                                    … except members of named group)
 (group = "<group name>");
```

Figure A-1. Sample ACL File Protecting 3 Resources (1 of 2)

```
acl "path=<fully qualified file name 3>";
authenticate (user,group) {
        database = "default";
        method = "basic";
};
deny (all)                                      (disallows access to file for everyone…
 (user = "all");

allow (all)                                     … except members of named group)
 (group = "<group name>");
```

Figure A-1. Sample ACL File Protecting 3 Resources (2 of 2)